# Posudek oponenta závěrečné práce

**České vysoké učení technické v Praze** **Fakulta informačních technologií**

**Student:** Bc. Jan Trusina
**Oponent práce:** Ing. Josef Kokeš
**Název práce:** Bezpečnostní studie aplikace
**Obor:** Počítačová bezpečnost

**Datum vytvoření:** 22. 5. 2017

| *Hodnotící kritérium:* | *Způsob hodnocení - následující škálou 1 až 5:* |
|---|---|
| **1. Náročnost a další komentář k zadání** | *1=mimořádně náročné zadání,*<br>*2=náročnější zadání,*<br>***3=průměrně náročné zadání,***<br>*4=lehčí, ale ještě dostatečně náročné zadání,*<br>*5=nedostatečně náročné zadání* |
| *Popis kritéria:*<br>Podrobněji charakterizujte diplomovou (bakalářskou) práci a její případné návaznosti na předchozí nebo běžící projekty. Dále posuďte, čím je zadání této ZP náročné. (U obtížnější ZP lze dále tolerovat některé nedostatky, které by u ZP standardní obtížnosti tolerovány nebyly; a naopak u jednoduché ZP mohou být zjištěné nedostatky hodnoceny přísněji.) | |
| *Komentář:*<br>Zadání týkající se reverzního inženýrství bývají obvykle spíše náročnější. Zaměření tohoto konkrétního zejména na připojení aplikace k internetu však v rámci problematiky patří k jednodušším. Přesto vztáhneme-li ho k tématům na FITu celkově, jde stále o průměrně nebo mírně nadprůměrně náročné zadání. | |

| *Hodnotící kritérium:* | *Způsob hodnocení - následující škálou 1 až 4:* |
|---|---|
| **2. Splnění zadání** | ***1=zadání splněno,***<br>*2=zadání splněno s menšími výhradami,*<br>*3=zadání splněno s většími výhradami,*<br>*4=zadání nesplněno* |
| *Popis kritéria:*<br>Posuďte, zda předložená ZP splňuje zadání. V komentáři uveďte body zadání, které nebyly zcela splněny, případně rozšíření ZP oproti původnímu zadání. Nebylo-li zadání zcela splněno, pokuste se posoudit závažnost, dopady a případně i příčiny jednotlivých nedostatků. | |
| *Komentář:*<br>Zadání bylo splněno. | |

| *Hodnotící kritérium:* | *Způsob hodnocení - následující škálou 1 až 4:* |
|---|---|
| **3. Rozsah písemné zprávy** | ***1=splňuje požadavky,***<br>*2=splňuje požadavky s menšími výhradami,*<br>*3=splňuje požadavky s většími výhradami,*<br>*4=nesplňuje požadavky* |
| *Popis kritéria:*<br>Zhodnoťte přiměřenost rozsahu předložené ZP vzhledem k obsahu, tj. zda všechny části ZP jsou informačně bohaté a ZP neobsahuje zbytečné části. | |
| *Komentář:*<br>Rozsah zprávy i hustota jejího obsahu jsou přiměřené. | |

| *Hodnotící kritérium:* | *Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **4. Věcná a logická úroveň práce** | *90 (A)* |
| *Popis kritéria:*<br>Posuďte, zda předložená ZP je po věcné stránce v pořádku, případně vyskytují-li se v práci věcné chyby nebo nepřesnosti. Zhodnoťte dále logickou strukturu ZP, návaznosti jednotlivých kapitol a pochopitelnost textu pro čtenáře. | |

*Komentář:*
Po věcné stránce je práce z velké většiny v pořádku. Popisované postupy jsou rozumné a vedou k výsledkům.

Nejzávažnější výhrady mám k sekci 5.5, kde zřejmě student myslel "digitální podpis", ale napsal "haš" (hash); i kvůli tomu jsou ve své odevzdané podobě doporučení 3 až 5 nefunkční a doporučení 6 nekompletní (je nutné testovat i certifikát serveru s XML souborem popisujícím dostupnost aktualizací). Celkově možná byly analýza i útok zastaveny příliš brzy, takže byl student sveden k neospravedlněným závěrům o a) jednoduchosti provedení plného útoku a b) účinnosti navrhovaných protiopatření.

Další věcné výhrady už jsou drobnější a uvádím je jen pro kompletnost:

- V analýze bych doporučoval zkoumat změny na celém disku C:, v sekci 3.2.3 např. velmi chybí %ALLUSERSPROFILE% a bylo by vhodné zkoumat i celý %USERPROFILE%.
- V sekci 3.2.5 se na straně 20 se hovoří o složkách se sníženými právy a myslí se tím složky, kam může uživatel zapisovat - to bych označil spíš jako zvýšená práva (nebo snížená omezení). Chybí mi vyjádření k právům ve složce C:\Kappa; pokud nebyla zaznamenána žádná změna jejích práv, tak jsou zde implicitně práva velmi vysoká, minimálně od Windows 7 výše dovolují zápis skupině AUTHENTICATED USERS.
- V sekci 3.3.3 jsou privilegia tokenu označena jako "standardní". K čemu aplikace potřebuje oprávnění Shutdown, Undock, TimeZone, viditelná na obrázku?
- U tabulky 3.1 by mělo být zdůvodnění jednotlivých závažností, zejména u metrik C, I, A. Nyní to vypadá, že jsou H a L přiřazena čistě subjektivně.

Logická stránka je v pořádku, velmi oceňuji shrnutí za každým rozsáhlejším celkem analýzy. Ta hodně pomáhají porozumění textu a orientaci v něm.

| *Hodnotící kritérium:* | *Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **5. Formální úroveň práce** | *85 (B)* |

*Popis kritéria:*
Posuďte správnost používání formálních zápisů obsažených v práci. Posuďte typografickou a jazykovou stránku ZP, viz Směrnice děkana č. 14/2015, článek 3.

*Komentář:*
Formální zápisy jsou vesměs bez problémů, velmi však chybí identifikace cíle odkazů - běžně je použit pouze odkaz bez identifikace jeho typu, takže čtenář neví, jestli se má dívat na kapitolu, obrázek, tabulku, algoritmus atd. (např. sekce 3.3.5.6, ale i mnoho dalších).

Po jazykové stránce je práce vysoce nadprůměrná, i když chyby stále obsahuje. Zvlášť nepříjemný je chybný pád v názvu sekce 2.1. Jinak jde vesměs o chyby v diakritice (chybějící háček, čárka) nebo překlepy. Subjektivně mi vadilo číst text v budoucím času první osoby množného čísla. Anglický abstrakt by si zasloužil korekturu.

| *Hodnotící kritérium:* | *Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **6. Práce se zdroji** | *70 (C)* |

*Popis kritéria:*
Vyjádřete se k aktivitě studenta při získávání a využívání studijních materiálů k řešení ZP. Charakterizujte výběr studijních pramenů. Posuďte, zda student využil všechny relevantní zdroje nebo zda se pokoušel řešit již vyřešené problémy. Ověřte, zda jsou všechny převzaté prvky řádně odlišeny od vlastních výsledků a úvah, zda nedošlo k porušení citační etiky a zda jsou bibliografické citace úplné a v souladu s citačními zvyklostmi a normami.

*Komentář:*
Práce důsledně cituje použité zdroje, bohužel až příliš. Ze skoro 70 unikátních odkazů je značná část v podstatě zbytečná a slouží pouze k vysvětlení nějakého pojmu, ne k doložení myšlenek (podle rychlého propočtu je v textu celkem 103 odkazů, z toho 82 jen na definice termínů). Nepovažuji za vhodné, aby po každém výskytu termínu následoval odkaz na zdroj, ve kterém se čtenář o tomto termínu může dozvědět více. Když už, tak toto má být součástí poznámek pod čarou, eventuálně samostatné sekce v bibliografii. Totéž platí o odkazech na použité nástroje. Skutečně použité zdroje se totiž v tom množství ztrácejí, navíc takové množství irelevantních odkazů působí při čtení velmi rušivě.

| *Hodnotící kritérium:* | *Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **7. Hodnocení výsledků, publikační výstupy a ocenění** | *90 (A)* |

*Popis kritéria:*
Vyjádřete se k úrovni dosažených hlavních výsledků ZP, např. k úrovni teoretických výsledků, nebo k úrovni a funkčnosti technického nebo programového vytvořeného řešení, apod. Případně také zhodnoťte, zda software nebo zdrojové texty, které nevytvořil sám student, byly v ZP použity v souladu s licenčními podmínkami a autorským právem. Popište případnou publikační činnost a získaná ocenění související s řešením této ZP.

*Komentář:*
Dosažené výsledky jsou velmi zajímavé. Studentovi se podařilo pochopit aplikaci do té míry, že v ní dokázal nalézt zranitelnost, a závažnost této zranitelnosti demonstroval útokem, který ji využije ke spuštění vlastního kódu, aniž by měl uživatel možnost si této skutečnosti všimnout. To lze jednoznačně hodnotit jako zásadní nedostatek v hodnocené aplikaci a student jeho nalezením prokázal, že si osvojil teorii i praxi problematiky bezpečnosti aplikací.

| *Hodnotící kritérium:* | *Způsob hodnocení - nehodnotí se* |
|---|---|
| **8. Komentář o využitelnosti výsledků** | |

Popis kritéria:
Uveďte, zda hlavní výsledky ZP rozšiřují již publikované známé výsledky a/nebo přinášející zcela nové poznatky. Uveďte možnosti využití výsledků ZP v praxi.

*Komentář:*

Využitelnost výsledků práce je bohužel v podobě, v jaké byla práce odevzdána, minimální. Příčinou je důsledné utajení jména aplikace, kvůli kterému uživatelé z analýzy získali pouze pocit ohrožení a doporučení, ať u postižené aplikace vypnou automatické aktualizace a provádějí aktualizace ručně z ověřeného serveru. To je za prvé bezpečnostně pochybné a za druhé to stejně nejde realizovat, když není známo, o kterou aplikaci se jedná. Skutečný přínos tak nastane až v okamžiku, kdy výrobce chybu opraví.

Existujícím přínosem je, že analýza podává návod, jak provádět další podobné analýzy. To není zanedbatelné.

| *Hodnotící kritérium:* | *Způsob hodnocení - nehodnotí se* |
|---|---|

**9. Otázky k obhajobě**

*Popis kritéria:*
Uveďte případné dotazy, které by měl student zodpovědět při obhajobě ZP před komisí (body oddělte odrážkami).

*Otázky:*

Máte nějakou zpětnou vazbu od výrobce, jak hodlá s nalezenou zranitelností naložit?

| *Hodnotící kritérium:* | *Způsob hodnocení - bodové hodnocení 0 až 100 bodů (známka A až F):* |
|---|---|
| **10. Celkové hodnocení** | *90 (A)* |

*Popis kritéria:*
Shrňte stránky ZP studenta, které nejvíce ovlivnily Vaše celkové hodnocení. Celkové hodnocení **nemusí** být aritmetickým průměrem či jinou hodnotou vypočtenou z hodnocení v předchozích jednotlivých kritériích 1 až 9.

*Text hodnocení:*

Práce samotná i přes jisté nedostatky v bodech 4 a 5 může být hodnocena jako výborná. Analýza byla provedena na vysoké úrovni a proof-of-concept útoku je přesvědčivý. Student tak úspěšně demonstruje, že si osvojil znalosti potřebné pro úspěšnou práci v tomto oboru. Subjektivně mám velký problém se sníženou využitelností výsledků pro uživatele (bod 8), uznávám ale důvody, které vedly k volbě tohoto řešení.

Podpis oponenta práce: